CONFLICT PREVENTION IN THE INFORMATION AGE
— ROLE OF MILITARY IN CRISIS —

BY

COLONEL GORO MATSUMURA
INTERNATIONAL FELLOW, JAPAN

USAWC CLASS OF 2001

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

20010622 083

Conflict Prevention in the Information Age
- Role of Military in Crisis -

by

COL Goro Matsumura
International Fellow, Japan

Dr. Steven Metz
Project Advisor

The views expressed in this academic research paper are those of the author and do not necessarily reflect the official policy or position of the U.S. Government, the Department of Defense, or any of its agencies.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Goro Matsumura

TITLE: Conflict Prevention in the Information Age – Role of Military in Crisis -

FORMAT: Strategy Research Project

DATE: 30 March 2001   PAGES: 36   CLASSIFICATION: Unclassified

What kind of military measures may be effective to prevent crisis from developing into armed conflict in the information age? How should military prepare for that mission? To answer these questions, it is indispensable to analyze the nature of armed conflicts in the information age. In this new age, an aggressor may be a non-state actor and may employ various asymmetrical measures. This new reality will change the calculations for deterrence. Technological or psychological surprise may perform a greater role. Manipulation of information by an aggressor may affect international or domestic public opinion in a greater degree. The situation may be developed too quickly to be followed by key decision makers. Development of new military technologies will raise numerous new ethical problems. Upon the analysis of these new approaches to war, the following three measures are recommended.
1. Establishment of "International Information Analysis Center for Conflict Prevention"
2. "Double Track Approach" including extensive R&D efforts and establishment of international arms control regimes for new military technologies
3. Active application of Non-lethal Weapons

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

LIST OF TABLES

CONFLICT PREVENTION IN THE INFORMATION AGE
- ROLE OF MILITARY IN CRISIS -

In March of 1996, China announced intentions to conduct three-phased large-scale joint exercise in vicinity of Taiwan in order to intimidate the first direct democratic election for the president of Taiwan. Some media reported that that China might commit a limited invasion on an isolated Taiwanese island to demonstrate their strong intent not to permit the independence of Taiwan. In response, the United States sent two aircraft carriers, Nimitz and Independence, to this area to demonstrate the U.S. will to defend Taiwan. Facing this powerful and clear response by the United States, China reduced the size of exercises and the invasion did not occur. The "show of force" operation by the two carriers succeeded.

But, in the 21st Century, will aircraft carriers still be effective tools for a "show of force"? Won't they be too vulnerable in an age when long-range precision strikes are common features of war? This paper examines which military measures may be effective to prevent crisis from developing into armed conflict in the information age and recommend how to prepare for that.

In this paper, the phrase "the information age" means the era in which a society in each country and the world system as a whole, has changed dramatically as a result of the information revolution. The information revolution is primarily caused by rapid development of information technologies represented by digitization and networking, but is closely related to the development in other technological areas such as biotechnology, nano-technology, space technology and so on. In the military arena, this change is called the Revolution in Military Affairs (RMA) or Information-based RMA.[1] This paper will refer to the 2020 time frame, when the information age is at hand.

"Conflict Prevention in the Information Age" is the primary issue of this paper. But all possible measures to prevent conflicts, for example, political, diplomatic, economic and cultural approaches, will not be discussed. This paper will discuss what military forces can do to prevent conflict. Military forces can contribute during peacetime, crisis, and post-conflict situations. In peacetime, they play a role in confidence building and a range of engagement activities, including helping developing states professionalize their armed forces through military to military contact. In post conflict situations, they can help rebuild

infrastructure and develop stability, both of which are important to prevent future conflict.[2] Although all of them are important roles, this study will specifically focus on the role of military during crisis.

The military effort for conflict prevention discussed in this paper is assumed to be a multinational activity. There will be several unilateral military measures employed to prevent conflicts. But those measures have to be coordinated as a whole in the international community or at least among several responsible countries. This is because the purpose of conflict prevention is to provide a stable global environment that equally benefits all nations in the world, not to achieve prosperity for one specific country.[3]

The first part of this paper will analyze the nature of armed conflicts in the information age and the difference from that of current or past conflicts. Next, the military role in conflict prevention in the information age will be examined to identify critical problems. Following the analysis of new military technologies applicable to solve these problems, recommendation will be made.

NATURE OF ARMED CONFLICTS IN THE INFORMATION AGE

It will be useful to categorize various armed conflicts in the information age into the following five categories in order to analyze their nature.

Category 1	Territorial invasion by digitized military
Category 2	Territorial invasion by hybrid military
Category 3	Escalation of long-standing dispute between countries
Category 4	Civil conflict
Category 5	Asymmetrical warfare

TABLE 1 CATEGORIES OF ARMED CONFLICTS IN THE INFORMATION AGE

TERRITORIAL INVASION BY A DIGITIZED MILITARY

The first category is a territorial invasion by a digitized military. In this case, a digitized military means armed forces which have dramatically improved C4I2 capabilities by utilizing the newest information technologies. These types of forces are occasionally called RMA forces. For example, we can imagine that

2

China has successfully digitized a considerable part of its armed forces by 2020 and may invade Taiwan with those forces. In another case, a restored Russia may have digitized military forces and invade Ukraine with them.

An invasion by a digitized military will be characterized by a short-term war with all high-tech measures. Quick victory in the short-term is the major concern of the invader. A country with a digitized military must be one of the highly developed countries in terms of economy. Otherwise it cannot afford to have an expensive digitized armed force. If so, the country's economic power inevitably depends on world economy. Leaders of invading country cannot ignore this fact when they conduct military operations. They will seek to conquer the territory they want in a short period and establish a *fait accompli* before other global powers intervene. The probability of this kind of invasion is very low. But if it occurs, it may cause a significant shift of power in the arena of international politics. We must be prepared to prevent it.

The most effective measure for short-term victory is a surprise attack. The aggressor can apply three techniques to achieve surprise. The first one is information dominance. This dominance will consist of the superiority of intelligence against a targeted country and an information shield isolating the theater from rest of the world. Superiority of intelligence is achieved by a highly-sophisticated information collecting and processing capability and deception capability including the utilization of sophisticated psycho-technology. An information shield will prevent other countries from understanding what really happens in the theater and keep them from intervening. Various countermeasures against the sensors deployed by other countries and cyber-attack against information collecting and processing systems of other countries will be used to establish this shield.

The second technique the aggressor may use to achieve surprise is a massive use of long-range precision guided weapons and sophisticated airlift capability. It is possible to attack a targeted country from dispersed positions with these technologies. In this case, it will be very difficult for other countries to catch signs of the invasion in advance.

The third technique is technological surprise. If an invading country utilizes one of the newest technologies in the world as a measure of offensive operations, it will be very difficult for other countries to immediately find a

countermeasure. Although it may be difficult to hide a new research and development program for a long time, it requires time and resources for other developed countries to develop a countermeasure to each new weapon. Furthermore, the invading country may synchronize applications of several new technologies, such as cyber-attack, long-range precise munitions, sophisticated special operations and psychological manipulation. Use of weapons of mass-destruction (WMD) does not seem to be highly possible in this case, because that will provoke world opinion and put the invading country in an unfavorable position following the war. Even invaders need to remain a part of the world economy system as an industrialized nation.

TERRITORIAL INVASION BY HYBRID MILITARY

Other potential aggressors such as Iraq, Iran or North Korea, may not have their armed forces digitized by 2020. Although they may have some weapons of mass destruction and some high-technology weapons, their main force will probably still be equipped with 20th Century type weapons. This type of territorial invasion by hybrid military is the second category.

A nation which tries to invade a neighbor without a digitized military must be prepared to fight two wars at the same time: a first war against the targeted country and a second war against the international community. Differing from a country with the digitized military of a global power, this aggressor may not have enough power to enforce the *fait accompli* gained by military invasion on the international community. Even though enough combat capability to defeat a targeted country can be massed, it will be difficult to repel international intervening forces including digitized military through conventional combat.

Aggressors can, however, apply some unconventional measures to make other countries, including global powers, to abandon intervention. The basic concept is to maximize cost of the intervention. For this purpose, aggressors may use WMD to inflict intolerable casualties on intervening forces or to deny access to major sea or airports into the theater. They may use a large number of special operation forces that may engage in sustained guerrilla combat to harass intervening forces. Or, aggressors may deploy hundreds of small missile boats to attack aircraft carriers or cargo ships. To make matters worse, they can take advantage of the so-called CNN effect in the information age. If deliberately

4

prepared psychological operations (PSYOPS) measures to manipulate public opinion in intervening countries are applied effectively, aggressors may succeed in deterring intervention or forcing intervening nations to withdraw.

ESCALATION OF LONG-STANDING DISPUTE

The third category is an intentional or accidental escalation of long-standing dispute between countries. This might involve countries like India and Pakistan over the Kashmir issue, or more than three, as in the territorial claims on the Spratly Islands. There are two different kinds of escalation of long-standing disputes. One is intentional escalation by one party, and another is accidental escalation. The nature of intentional escalation is almost similar to that of invasion.

If any minor unintentional collision between armed forces occurs in the area where a long-standing controversy, such as territorial claims from more than two countries exists, people in the countries concerned will be informed immediately about the incident by the media. Because the first news will probably be provided by domestic media in each country concerned, we can not expect an impartial reporting. A danger exists here. It is likely that each government concerned cannot calmly deal with the incident because of heated public opinion provoked by the media.

Before the information age, governments collected more information faster than ordinary citizens. In the information age, people are informed almost at the same time as their decision makers. The decision makers need time to analyze the situation carefully and develop the best course of action to protect their national interests. In many cases, avoiding armed conflict is a better way to achieve national goals than employing military force. Nevertheless, radical public opinion tends to develop faster than rational government decisions, and decision makers may be forced to react a public opinion because of dynamics of domestic politics.

The danger of accidental escalation increases when the involved governments do not have the capability to deal with the information coming at tremendous speed. They may have little time for rational analysis.

CIVIL CONFLICT

The fourth category of armed conflict in the information age is a civil conflict. In the early 21st Century, it is anticipated that the wave of globalization will sweep all countries in the world, change the nature of societies and force people a new lifestyle rapidly. As a reaction to this radical change, some people may want to reestablish their identity by emphasizing their unique ethnicity, religion or local culture. This movement will have a tendency to aggravate a local dispute in a country and may cause civil conflict. Increasing differences between the rich and the poor may destabilize a society and cause conditions that lead to a civil conflict.[4]

Civil conflicts in the information age are not genuine domestic issues any more. This is not only due to humanitarian concerns spread all over the world with the development of real-time broadcasting, but also due to the nature of globalization which cause a friction between globalizationalist and anti-globalizationalists, haves and have-nots or among have-nots.

Because of this nature, two opposite dynamics are at work on civil conflict of the information age. One is the frequent intervention from the international community, motivated by humanitarian or economic concerns. In order to develop a sound global economic system, stabilization of the world is indispensable. But there is another possible situation derived from the same concern. Countries that are already globalized and enjoying economic prosperity may try to maintain the stability of their system by isolating a destabilized country or region. This situation is not necessarily created intentionally by public opinion in developed countries. It is natural, in light of economic theory, that capital is withdrawn from a country with growing risk.[5] Economics often leads politics. A country afflicted by civil conflict may fall into a vicious cycle of internal confrontation and poor economy. So called "failed states" are often created through this process.[6] These nations will eventually destabilize the world through spillover of conflict, overflow of refugees or desperate aggressive actions.

A wide range of means, from axes and clubs to a cyber attack, will be used in the civil conflict of the information age. Psychological operations (PSYOP)

may also become an important factor through the use of psychological technology and manipulation of media.

ASYMMETRICAL WARFARE

The last category is unique and important in the information age. This category can be referred as an "asymmetrical warfare". In the first and second categories, leaders of invading countries make the decision to invade because they believe they have a stronger military than that of the invaded countries. But in this asymmetrical warfare, they may attack a stronger enemy by asymmetric means, such as terrorism, cyber attack or use of WMD including biological weapon, in order to achieve a limited political objective.[7] Making the matter worse, they may not be nation-states, but networked organizations.[8] It might be a network of international political groups led by a specific ideology, international narco-trafficking or other crime organizations, or even international black money brokers.[9] In the worst case, it might be impossible for the attacked country to identify the attacker. In the information age, it may be possible that the attacker is a network without any centralized head.

A key to success for the aggressors in asymmetrical warfare is technological surprise. If new measures are employed that are not anticipated by targeted countries, aggressors will possibly be able to cause panic and may achieve their political goal. For this purpose they can utilize a wide range of highly advanced technologies. In the area of cyber attack, they may find a new weakness beyond imagination because we are depending on computer networks more and more in every area of our lives. As for chemical and biological weapons, many new types of agents are becoming available by applying new biotechnology and/or the newest knowledge of cerebrum physiology. Aggressors may choose an agent that provokes public anxiety. In this case, chemical warfare becomes a measure of PSYOPS. They may use a micro-machine like a bug, made with the newest nano-technology, as a projector of such a chemical or biological agent. There are limitless possibilities.

If parties who attempt asymmetrical warfare are networks of various groups without any headquarters, the groups may attack independently but in a synchronized manner, by cooperating and complementing each other. High-technology weapons, such as stealth fighters or long-range precision attack

missiles, are becoming more expensive. On the other hand, application of high technology for civilian use, such as Internet or a cellular phone, is becoming increasingly less expensive. Even political or terrorist groups without money can develop unique weapons by utilizing the emerging new civilian technologies and communicate in real time to synchronize their actions by using commercial networks.

MILITARY ROLE IN CONFLICT PREVENTION IN THE INFORMATION AGE

GENERAL ROLE OF MILITARY IN CONFLICT PREVENTION

In the present condition, roles of military during crisis can be generally divided into four major areas: Information collection, preventive Peace Keeping Operations (PKOs), military actions for deterrence, and support for political/economical sanction.[10]

Armed forces have a wide variety of assets for military information gathering including satellites, reconnaissance aircraft, airborne/sea-based/land-based radar, SIGINT/ELINT devices and other technical means. Information collected by these assets is useful for an early warning of crisis in the international community and as a basis of cooperative political/economic/military measures to prevent conflict.

Preventive PKOs include the preventive deployment of Peace Keeping Forces, dispatch of military observers, creation of neutral zone observed by Peace Keeping Forces and any combination of these. They are usually deployed by the United Nations (UN), or other regional organizations, when the host nation has requested or agreed to the deployment. The US forces deployed in 1993 to Macedonia in support UN effort to limit the fighting in former Yugoslavia is a successful example of preventive deployment.

If the danger of invasion is emerging, allies of a targeted country or other countries supporting international peace can demonstrate their military capability to deter the invasion. This type of deterrence is distinguished as an "immediate deterrence" in a crisis, which is different from "general deterrence" in peacetime.[11] While general deterrence is achieved by a static balance of combat power, immediate deterrence is achieved by the dynamic movement or activities

of armed forces. Dispatching new forces, increasing show of force activities, deploying forces forward in the theater, increasing exercises and increasing reconnaissance activities are all measures of immediate deterrence. This type of military measures is similar to "Military Flexible Deterrence Options" stated in the US Armed Forces joint doctrine.[12]

In order to stop aggressive activities by a specific country, UN or other regional organizations may apply political or economic sanctions against the country. In such cases, the effectiveness of the sanction must be backed by military measures such as operations enforcing exclusion zones or maritime inspection operations.

Type of Operations	Examples
Information Collection	- Reconnaissance satellites/aircraft - airborne/sea-based/land-based radar - SIGINT/ELINT
Preventive PKOs	- preventive deployment of Peace Keeping Forces - dispatch of military observers mission - creation of neutral zone observed by Peace Keeping Forces
Immediate Deterrence	- dispatching new forces - increasing show of force activities - deploying forces forward in the theater - increasing exercises - increasing reconnaissance activities
Support to Sanctions	- operations enforcing exclusion zones - maritime inspection operations

TABLE 2 ROLE OF MILITARY IN CONFLICT PREVENTION

NEW ROLE OF MILITARY IN THE INFORMATION AGE

Preventing invasion by digitized military

Information gathering is an important military role in preventing invasion by a digitized military. In peacetime, we have to keep collecting information about the latest military technology in order to avoid technological surprise. In crisis, we need to have capabilities to break through the information shield set by a digitized enemy. Additionally, there is also great importance on gathering

information about an invader's intent by human resources intelligence (HUMINT), or other sophisticated measures.[13]

What can be done after collecting enough information to indicate the imminent danger of invasion? The military can provide the information to their government or international organizations, who will employ diplomatic or economic measures to prevent the invasion, or to media in order to form international public opinion against the invasion. At the same time, it is important to establish a favorable military posture for immediate deterrence as soon as possible. By doing so, a signal can be sent to the potential invader. Classical "show of force" may be a dangerous option because the invader has digitized forces with sophisticated long-range munitions. It seems to be effective to "show" our technological supremacy in some areas of intelligence and/or offensive capability. A type of demonstration that is not too provocative, such as signal interference, may be suitable for this purpose.

Preventing invasion by hybrid military

Information collection and immediate deterrence are also important military roles in the prevention of invasion by a hybrid military. Although information gathering against a hybrid military is probably easier when compared to that against a digitized military, it is a tougher job to deter the invasion by maintaining international resolve to fight against any illegal aggression. Aggressors may employ WMD attack or guerrilla warfare in order to intimidate the international community. Our military must be prepared to fight and win under any condition in order to maintain the credibility of deterrence. Both defensive and offensive counter-proliferation capabilities, such as ballistic missile defense and surgical strike capabilities, will be a part of these efforts. Furthermore, PSYOP and public affairs activities to acquire domestic and international support are indispensable to maintain the resolve of the international community.

Preventing an escalation of a long-standing dispute

Certainly preventive PKOs may be effective in preventing accidental escalation of long-standing disputes. At the same time, the open and continuous supply of real-time information and objective analysis, to the international community, will be effective in avoiding misunderstandings by any party

concerned. In particular, objective international analysis is important, because there is so much information available in the information age that each country cannot always possess sufficient information processing and analyzing capability.

Preventing civil conflict

The military role in preventing internal conflict is limited. Instead, political and/or economic efforts seem to perform a major role in this area. It is possible that a government, which does not have enough capability to suppress insurgency, may depend upon other countries or international organizations to provide military support. In such cases, preventive PKOs may be employed to prevent civil conflict. But, in many cases, even the government does not have enough legitimacy either because of corruption, violations of human rights or repression. Early warning based on robust information collection efforts may work. But, after the warning, it seems that the missions which the military can perform to prevent such conflict are very limited. The interception of incoming weapons into the country under an international arms control arrangement may be one of the limited missions.

Preventing asymmetrical warfare

In order to deter asymmetrical warfare, extensive military research and development (R&D) efforts to avoid any technological surprise are important. If an aggressor is confident that we do not have any countermeasure or protecting measures against his new weapon, the possibility of deterrence is minute. Even in cases that we have countermeasures, aggressors may still try to attack us. We may need a retaliatory capability to deter such an enemy.

Intelligence is also important in this type of war, not only for avoiding technological surprise but also for distinguishing the enemy. If the enemy is of a network type and does not have centralized command structure, we need a robust effort to find the enemy's center of gravity and determine where we should orient our operations. Information collection in cyber-space will be inevitable in this kind of intelligence effort.

MILITARY ISSUES IN CONFLICT PREVENTION IN THE INFORMATION AGE

IMPORTANCE OF INFORMATION ABOUT THE ENEMY'S INTENTION

In the information age, invaders can conceal their preparation for invasion to some extent, because they do not always need mass of force, instead taking advantage of long-range precision munitions and/or various asymmetric measures. Therefore, the collection of information concerning an enemy's intention will have a critical role in issuing a timely and effective early warning. For this reason, HUMINT is still, or maybe more, important in the information age. We need to develop new measures to collect information about an enemy's intent by applying advanced technologies. [14]

NECESSITY FOR OBJECTIVE INFORMATION ANALYSIS CAPABILITY

Objective analysis of information is very important in conflict prevention. There is a lot of information available in the information age. It is critical to select accurate and useful information and analyze it objectively. Otherwise, too much information may be misinterpreted and lead to an overreaction such as preemptive attack. In other cases, an invader may attempt to manipulate information to deceive the international community, or the international media may report a prejudiced view intentionally or unintentionally. Therefore, a database of objectively analyzed information about international disputes, accessible by every member in the international community, will provide a significant basis for the various efforts to prevent conflict.

NEED FOR A WIDE VARIETY OF CAPABILITIES TO AVOID TECHNOLOGICAL SURPRISE

Advanced technologies in the information age provide countries or groups attempting aggression with limitless potential. In order to deter and deal with these capabilities, responsible countries must proceed with military R&D programs in every technological area. At the same time, an international framework that controls the inhumane military application of advanced technologies must be sought.

NEW NATURE OF DETERRENCE IN THE INFORMATION AGE

During the Cold War, deterrence by punishment and deterrence by denial were mainly achieved by nuclear and conventional capabilities respectively.[15] Is the theory of deterrence still valid in the information age? If not, a new mechanism of deterrence should be developed in order to find appropriate military measures to prevent conflicts. [16]

If nuclear capability is the only a tool for deterrence by punishment, credibility of deterrence for less vital areas is inevitably low, because the threshold of nuclear use is high. In the information age, however, long-range precision strike capability may seem to be effective as a punishment tool, because it enables us to directly attack enemy's decision makers. So we may be able to expect a deterrence by punishment effect even in less vital areas. This is good news for conflict prevention. But there is also bad news. Terrorism by WMD or other asymmetric measures may be effective tools to deter the international community from intervening.

Deterrence by denial is becoming more difficult in the information age, because combat power is more dispersed and not necessarily visible in the theater. It is necessary to demonstrate that the international community, including responsible developed countries, is always watching and ready to intervene if necessary. It seems to be effective in crisis to send a signal to a potential aggressor by deploying sensors in the theater. This operation can be called the "show of sensor" instead of the "show of force".

HOW TO MAINTAIN CREDIBILITY OF INTERVENTION TO ENSURE DETERRENCE

If a potential aggressor underestimates the resolve of the international community to resist the aggression, deterrence does not work. Credibility of intervention is the key of effective deterrence. In order to maintain the credibility, it is essential that the governments participating in the intervention are supported by domestic public opinion in each country. If estimated friendly and/or collateral casualties are high, the governments will not be able to get enough public support and may hesitate to intervene. Therefore, an effort to reduce casualties is one of critical factors to ensure deterrence. Emerging new technologies in the information age may be able to contribute to this effort.

13

ETHICAL PROBLEMS BROUGHT BY NEW TECHNOLOGIES

While these applications of advanced technologies provide us significant capabilities to prevent conflict, they raise a new type of ethical problems.

- Deployment of micro-sensors into foreign territory or surveillance in cyber-space may violate the national sovereignty of other countries. Even if the governments of countries concerned agree those activities, these measures will possibly intrude on the right to protect personal privacy. We need a new international rule in order to employ those measures effectively.
- If the intelligence analysis provided by AI automatically is used to base an incorrect decision to go to war, who is responsible for that decision?
- Long-range precision strike is an effective tool to attack an enemy's center of gravity. But if the center is the enemy's political leader, the attack means an assassination. Is this a just war or a criminal activity?
- Non-lethal weapons and unmanned weapons will provide flexible options and enable rapid decision-making. But doesn't this mean a lower threshold of war and increased chance of war, rather than deterring war?[19]
- If unmanned weapons are widely used in the battlefield, only the enemy's-side has casualties and there is no human damage on our side. Is this ethically permitted? Isn't this massacre?

All of these questions should be answered in order to utilize these technologies with international legitimacy.

RECOMMENDATIONS

In order to validate effective international cooperation to prevent conflicts, the following three points are recommended to governments of responsible developed countries in the world.

INTERNATIONAL DATABASE PROVIDING OBJECTIVE MILITARY INTELLIGENCE

Objective military intelligence is very important for conflict prevention. It will provide the basis to issue early warning to the international community. It will achieve a significant role to avoid misunderstanding by each party concerned. It

will be an effective tool to neutralize PSYOPS or information manipulation conducted by an aggressor. It will provide common recognition when multinational military operations to prevent conflicts are planned and executed.

Whatever it is, multilateral framework for information collection, processing and analysis will achieve a significant role for conflict prevention in the information age. One of the best approaches is to establish an "International Information Analysis Center for Conflict Prevention". Although participation from a number of countries is not necessarily required to establish this center, participation from several responsible developed countries is necessary to avoid excessive dependence on any single information source. Information will be collected by assets owned and operated by each participant and offered to the center on voluntary basis. Responsible, developed nation should willingly contribute to this framework.

There are three keys to the success of this center. First, processing and analysis must be done multilaterally to ensure objectivity and impartiality. Second, the output must be open to not only participating countries but also all parties requiring the information. Third, real-time information processing and analyzing capability is indispensable in keeping pace with a rapidly changing situation in crisis and provide timely the necessary intelligence. Although it is desirable to establish the center as a standing organization, it is also possible to create an ad-hoc framework for a multinational cooperation to analyze information to prevent a specific conflict.

"DOUBLE TRACK" APROACH
EXTENSIVE R&D EFFORT AND INTERNATIONAL ARMS CONTROL REGIMES

In order to decrease the possibility of a technical surprise by an aggressor, robust R&D programs concerning the application of various advanced technologies for the military are indispensable. Efforts by responsible developed countries are critical in forestalling potential aggressors, rogue states or international crime organizations. Specialization among developed countries having sufficient mutual trust each other may work well to progress an R&D program in a wide area with limited resources. At the same time, the effort to

17

establish international regimes to control those advanced technology weapons is significantly important because of following three reasons.

First, there are technologies to which application for military purpose may cause seriously hazardous effects on human beings. Biotechnology, psycho-technology, advanced medical technology or meteorological technology may be such areas. We need an international regime in order to force potential aggressors not to acquire those kinds of weapons.[20] We will be able to gain legitimacy to enforce a rule even when the regime is not perfect. We can apply internationally legitimate sanctions against Iraq and North Korea because they are members of the Nuclear Non-Proliferation Treaty (NPT). Without the treaty, we cannot have the legitimacy.

Second, there are technologies which utilization by one country may cause ethical problems even if those technologies favor international conflict prevention. If micro-sensors to collect information about aggressor's intent, long-range precise strike on specific enemy leaders or unmanned weapons which fight automatically upon enemy's attack are employed by one specific country, they will cause an ethical controversy domestically or internationally. Their employment under authorization by the international communities will ease that kind of argument.

Third, the R&D by developed countries may cause suspicion and distrust in developing countries. It is important the regimes are managed by the international community, including the responsible developing countries.

APPLICATION OF NON-LETHAL WEAPONS

Rapid response with enough power is critical to prevent a full-scale armed conflict when an incident involving some level of violence occurs in a disputed area. But reality tells us that military commitments from outside tend to be too late, because foreign governments as third party are afraid of collateral casualties or excessive provocative effect by using military forces. If there is any tool which is more powerful than observers and less provocative than fully equipped troops, that will enable quicker commitment from outside to stabilize the situation. Non-lethal weapons provide that kind of capability. Rapid deployment of unilateral or multilateral forces equipped with non-lethal weapons

will provide the international community with another flexible option to prevent an armed conflict in crisis.

Non-lethal weapons are also useful as signaling or warning measures to deter potential invasions. This type of capability is important when an invasion is imminent. It is critical to deter or limit the invasion in an early stage by sending strong message concerning to the strong resolve and enough capability to defeat the aggressor. Non-lethal weapons are appropriate assets to show an attacking capability based on superior intelligence. Retaliation capability can be shown by attacking their political or command and control center precisely with a non-lethal weapon. Or, denial capability can be shown by attacking their front troops. By providing these kinds of flexible options, non-lethal weapons have effect of lowering threshold of intervention and making deterrence more credible.

Of course, there is also a negative aspect of the use of non-lethal weapons. Governments of major countries may be tempted to use force more easily with less consideration.[21] That may increase conflicts instead of preventing them. In order to avoid this side effect, establishment of international rules about use of non-lethal weapons and/or creation of a certain kind of international regime to control them will be necessary.

WORD COUNT = 5950

ENDNOTES

[1] Gregory J. Rattray and Laurence E. Rothenberg, "A Framework for Discussing War in the Information Age," in War in the Information Age: New Challenges for U.S. Security Policy, eds. Robert L. Pfaltzgraff, Jr. and Richard H. Shultz,Jr, (Washington D.C.: Brassey's, 1997): 343.

[2] Michael S. Lund, Preventing Violent Conflicts: A Strategy for Preventive Diplomacy, (Washington, D.C.: United States Institute of Peace Press,1996), 37-44.

[3] Ibid., 169.

[4] Thomas L. Friedman, The Lexus and the Olive Tree, (New York: Anchor Books, 2000), 344-346.

[5] Ibid., 112-142.

[6] Robert H. Dorff, "Responding to the Failed State: The Need for Strategy," Small Wars and Insurgencies, Vol.10, No.3 (Winter 1999): 65.

[7] Joint Vision 2020, (Washington, D.C.: The Joint Staff, June 2000),5.

[8] Steven Metz and Douglas V. Johnson II, Asymmetry and U.S. Military Strategy: Definition, Background, and Strategic Concepts, (Carlisle Barracks: Strategic Studies Institute, 2001),14.

[9] Edwin G. Corr and Max G. Manwaring, "The Challenge of Preventive Diplomacy and Deterrence in Global Security Environment: Applying the 'Iron Fist' within the 'Velvet Glove' Now and in the Future" in Deterrence in the 21st Century. ed. Max G. Manwaring, (London / Portland, OR: Frank Cass, 2001),127.

[10] Daniel J. Kaufman, "The Role of the Military in Preventing Deadly Conflict" in Preventing Deadly Conflict: Strategies and Institutions, eds. Gail W. Lapidus

and Svetlana Tsalik, (New York: Carnegie Corporation of New York, 1998), 145-147.

[11] Patrick M. Morgan, <u>Deterrence: A Conceptual Analysis,</u> (Beverly Hills, CA: Sage Publications, Inc., 1977), 28-29.

[12] <u>The Joint Staff Officer's Guide 2000,</u> JFSC PUB 1, (National Defense University, Joint Forces Staff College,2000), 4.20-24.

[13] <u>Road Map for National Security: Imperative for Change,</u> (The United States Commission on National Security/21st Century, January 31, 2001), 82-82.

[14] Ibid., 85.

[15] Glenn H. Snyder, <u>Deterrence by Denial and Punishment,</u> (Center of International Studies, Princeton University, 1958), 2.

[16] Robert H. Dorff and Joseph R. Cerami, "Deterrence and Competitive Strategies: A New Look at an Old Concept" in <u>Deterrence in the 21st Century,</u> ed. Max G. Manwarning, (London / Portland, OR: Frank Cass, 2001), 109-117.

[17] Steven Metz, <u>Armed Conflict in the 21st Century: The Information Revolution and Post-Modern Warfare,</u> (Carlisle Barracks: Strategic Studies Institute, 2000), 66-68.

[18] Ibid., 77-79.

[19] Joseph Siniscalchi, <u>Non-lethal Technologies: Implications for Military Strategy,</u> (Maxwell Air Force Base: Air University, 1998), 23-25.

[20] Steven Metz, "Racing Toward the Future: The Revolution in Military Affairs." <u>Current History</u> (April 1997), 188.

[21] Douglas C. Lovelace Jr. and Steven Metz, <u>Nonlethality and American Land Power: Strategic Concept and Operational Concepts,</u> (Carlisle Barracks: Strategic Studies Institute, 1998), 12.

BIBLIOGRAPHY

FUTURE WARFARE

Metz, Steven. Armed Conflict in the 21st Century: The Information Revolution and Post-Modern Warfare. Carlisle Barracks: Strategic Studies Institute, 2000.

Pfaltzgraff, Robert L. Jr., and Richard H. Shultz,Jr, eds. War in the Information Age: New Challenges for U.S. Security Policy. Washington D.C.: Brassey's, 1997.

Leonhard, Robert R. The Principles of War for the Information Age. Novato, CA: Presidio Press, 1998.

Copeland, Thomas E. ed. The Information Revolution and National Security. Carlisle Barracks: Strategic Studies Institute, 2000.

Henry, Ryan, and C. Edward Peartree, eds. The Information Revolution and International Security. Washington, D.C.: The CSIS Press, 1998.

McCarthy, James P., ed. National Security in the Information Age. Colorado: US Air Force Academy, 1996

Metz, Steven. "Racing Toward the Future: The Revolution in Military Affairs." Current History April 1997: 184-188.

Metz, Steven, and Douglas V. Johnson II. Asymmetry and U.S. Military Strategy: Definition, Background, and Strategic Concepts. Carlisle Barracks: Strategic Studies Institute, 2001.

PREVENTIVE DIPLOMACY

Lund, Michael S. Preventing Violent Conflicts: A Strategy for Preventive Diplomacy. Washington, D.C.: United States Institute of Peace Press,1996.

Lapidus, Gail W., and Svetlana Tsalik, eds. Preventing Deadly Conflict: Strategies and Institutions. New York: Carnegie Corporation of New York, 1998.

DETERRENCE

Manwarning, Max G., ed. Deterrence in the 21st Century. London / Portland, OR: Frank Cass, 2001.

Snyder, Glenn H. Deterrence by Denial and Punishment. Center of International Studies, Princeton University, 1958.

Morgan, Patrick M. Deterrence: A Conceptual Analysis. Beverly Hills, CA: Sage Publications, Inc., 1977.

NON-LETHAL WEAPONS

Lovelace, Douglas C. Jr., and Steven Metz. Nonlethality and American Land Power: Strategic Concept and Operational Concepts. Carlisle Barracks: Strategic Studies Institute, 1998.

Metz, Steven. "Non-lethality and the Revolution in Military Affairs." In Non-lethal Weapons: Technological and Operational Prospects, ed. Malcolm Dando. Jane's Information Group,2000.

Siniscalchi, Joseph. Non-lethal Technologies: Implications for Military Strategy. Maxwell Air Force Base: Air University, 1998.

MISCELLANEOUS

Dorff, Robert H. "Responding to the Failed State: The Need for Strategy." Small Wars and Insurgencies, Vol.10, No.3 (Winter 1999). 62-81.

Nye, Joseph S. Jr. National Interest in the Information Age. New York: Carnegie Council, 1999.

Friedman, Thomas L. The Lexus and the Olive Tree. New York: Anchor Books, 2000.